CSP

5
68%

Table 1

Security SAFEGUARDS by Mode of Operation

SAFEGUARD	Dedicated	System High	Compartmented	Multilevel *
Access Control and Labels				
1. Discretionary Access Control	A	A	A	A
2. Object Reuse	—	—	A	A
3. Labels	A	A	A	A
4. Mandatory Access Control	A	A	A	A
Accountability				
5. Identification & Authentication	A	A	A	A
6. Identification of User Terminal	—	A	A	A
7. Trusted Path	—	A	A	A
8. Audit	—	A	A	A
Operational Assurance				
9. System Architecture	—	A	A	A
10. System Integrity	—	A	A	A
11. Trusted Facility Management	—	A	A	A
12. Trusted Recovery	—	—	A	A
Life Cycle Assurance				
13. Security Testing	—	A	A	A
14. Design Specification & Verification	—	—	A	A
15. Configuration Management	—	A	A	A
16. Trusted Distribution	—	A	A	A
Documentation				
17. System Security Statement/Plan	A	A	A	A
18. Security Features User's Guide	A	A	A	A
19. Trusted Facility Manual	—	A	A	A
20. Test Documentation	—	A	A	A
21. Design Documentation	—	—	A	A
Environmental Protection				
22. Communications Security (COMSEC)	A	A	A	A
23. Physical Security	A	A	A	A
24. TEMPEST	A	A	A	A
25. Personnel Security	A	A	A	A
Administrative				
26. Annual Accreditation	A	A	A	A
27. Dial-up Lines	A	A	A	A
28. Protection of Software	A	A	A	A
29. Access Authentication	A	A	A	A

Note: "A" means applicable to the identified modes of operation.

* Although the requirements for the compartmented and multilevel modes of operation are essentially the same, there are some additional procedures required for the latter. The most significant difference is that the DCI is the accreditation authority for systems and networks operating in the multilevel mode. (UNCLASSIFIED)

MAXI

Table 1

Security SAFEGUARDS by Mode of Operation

SAFEGUARD	Dedicated	System High	Compartmented	Multilevel *
Access Control and Labels				
1. Discretionary Access Control	A	A	A	A
2. Object Reuse	—	—	A	A
3. Labels	A	A	A	A
4. Mandatory Access Control	A	A	A	A
Accountability				
5. Identification & Authentication	A	A	A	A
6. Identification of User Terminal	—	A	A	A
7. Trusted Path	—	A	A	A
8. Audit	—	A	A	A
Operational Assurance				
9. System Architecture	—	A	A	A
10. System Integrity	—	A	A	A
11. Trusted Facility Management	—	A	A	A
12. Trusted Recovery	—	—	A	A
Life Cycle Assurance				
13. Security Testing	—	A	A	A
14. Design Specification & Verification	—	—	A	A
15. Configuration Management	—	A	A	A
16. Trusted Distribution	—	A	A	A
Documentation				
17. System Security Statement/Plan	A	A	A	A
18. Security Features User's Guide	A	A	A	A
19. Trusted Facility Manual	—	A	A	A
20. Test Documentation	—	A	A	A
21. Design Documentation	—	—	A	A
Environmental Protection				
22. Communications Security (COMSEC)	A	A	A	A
23. Physical Security	A	A	A	A
24. TEMPEST	A	A	A	A
25. Personnel Security	A	A	A	A
Administrative				
26. Annual Accreditation	A	A	A	A
27. Dial-up Lines	A	A	A	A
28. Protection of Software	A	A	A	A
29. Access Authentication	A	A	A	A

59%

Note: "A" means applicable to the identified modes of operation.

* Although the requirements for the compartmented and multilevel modes of operation are essentially the same, there are some additional procedures required for the latter. The most significant difference is that the DCI is the accreditation authority for systems and networks operating in the multilevel mode. (UNCLASSIFIED)

K AIS

Table 1

Security SAFEGUARDS by Mode of Operation

SAFEGUARD	Dedicated	System High	Compartmented	Multilevel *
Access Control and Labels				
1. Discretionary Access Control	A	A	A	A
2. Object Reuse	—	—	A	A
3. Labels	A	A	A	A
4. Mandatory Access Control	A	A	A	A
Accountability				
5. Identification & Authentication	A	A	A	A
6. Identification of User Terminal	—	A	A	A
7. Trusted Path	—	A	A	A
8. Audit	—	A	A	A
Operational Assurance				
9. System Architecture	—	A	A	A
10. System Integrity	—	A	A	A
11. Trusted Facility Management	—	A	A	A
12. Trusted Recovery	—	—	A	A
Life Cycle Assurance				
13. Security Testing	—	A	A	A
14. Design Specification & Verification	—	—	A	A
15. Configuration Management	—	A	A	A
16. Trusted Distribution	—	A	A	A
Documentation				
17. System Security Statement/Plan	A	A	A	A
18. Security Features User's Guide	A	A	A	A
19. Trusted Facility Manual	—	A	A	A
20. Test Documentation	—	A	A	A
21. Design Documentation	—	—	A	A
Environmental Protection				
22. Communications Security (COMSEC)	A	A	A	A
23. Physical Security	A	A	A	A
24. TEMPEST	A	A	A	A
25. Personnel Security	A	A	A	A
Administrative				
26. Annual Accreditation	A	A	A	A
27. Dial-up Lines	A	A	A	A
28. Protection of Software	A	A	A	A
29 Access Authentication	A	A	A	A

71%

Note: "A" means applicable to the identified modes of operation.

* Although the requirements for the compartmented and multilevel modes of operation are essentially the same, there are some additional procedures required for the latter. The most significant difference is that the DCI is the accreditation authority for systems and networks operating in the multilevel mode. (UNCLASSIFIED)

VDSC

58%

Table 1

Security SAFEGUARDS by Mode of Operation

SAFEGUARD	Dedicated	System High	Compartmented	Multilevel *
Access Control and Labels				
1. Discretionary Access Control	A	A	A	A
2. Object Reuse	—	—	A	A
3. Labels	A	A	A	A
4. Mandatory Access Control	A	A	A	A
Accountability				
5. Identification & Authentication	A	A	A	A
6. Identification of User Terminal	—	A	A	A
7. Trusted Path	—	A	A	A
8. Audit	—	A	A	A
Operational Assurance				
9. System Architecture	—	A	A	A
10. System Integrity	—	A	A	A
11. Trusted Facility Management	—	A	A	A
12. Trusted Recovery	—	—	A	A
Life Cycle Assurance				
13. Security Testing	—	A	A	A
14. Design Specification & Verification	—	—	A	A
15. Configuration Management	—	A	A	A
16. Trusted Distribution	—	A	A	A
Documentation				
17. System Security Statement/Plan	A	A	A	A
18. Security Features User's Guide	A	A	A	A
19. Trusted Facility Manual	—	A	A	A
20. Test Documentation	—	A	A	A
21. Design Documentation	—	—	A	A
Environmental Protection				
22. Communications Security (COMSEC)	A	A	A	A
23. Physical Security	A	A	A	A
24. TEMPEST	A	A	A	A
25. Personnel Security	A	A	A	A
Administrative				
26. Annual Accreditation	A	A	A	A
27. Dial-up Lines	A	A	A	A
28. Protection of Software	A	A	A	A
29. Access Authentication	A	A	A	A

Note: "A" means applicable to the identified modes of operation.

* Although the requirements for the compartmented and multilevel modes of operation are essentially the same, there are some additional procedures required for the latter. The most significant difference is that the DCI is the accreditation authority for systems and networks operating in the multilevel mode. (UNCLASSIFIED)

CIRC

3.4
6 8

Table 1

Security SAFEGUARDS by Mode of Operation

7670

SAFEGUARD	Dedicated	System High	Compartmented	Multilevel *
Access Control and Labels				
1. Discretionary Access Control	A	A	A	A
2. Object Reuse	—	—	A	A
3. Labels	A	A	A	A
4. Mandatory Access Control	A	A	A	A
Accountability				
5. Identification & Authentication	A	A	A	A
6. Identification of User Terminal	—	A	A	A
7. Trusted Path	—	A	A	A
8. Audit	—	A	A	A
Operational Assurance				
9. System Architecture	—	A	A	A
10. System Integrity	—	A	A	A
11. Trusted Facility Management	—	A	A	A
12. Trusted Recovery	—	—	A	A
Life Cycle Assurance				
13. Security Testing	—	A	A	A
14. Design Specification & Verification	—	—	A	A
15. Configuration Management	—	A	A	A
16. Trusted Distribution	—	A	A	A
Documentation				
17. System Security Statement/Plan	A	A	A	A
18. Security Features User's Guide	A	A	A	A
19. Trusted Facility Manual	—	A	A	A
20. Test Documentation	—	A	A	A
21. Design Documentation	—	—	A	A
Environmental Protection				
22. Communications Security (COMSEC)	A	A	A	A
23. Physical Security	A	A	A	A
24. TEMPEST	A	A	A	A
25. Personnel Security	A	A	A	A
Administrative				
26. Annual Accreditation	A	A	A	A
27. Dial-up Lines	A	A	A	A
28. Protection of Software	A	A	A	A
29. Access Authentication	A	A	A	A

Note: "A" means applicable to the identified modes of operation.

* Although the requirements for the compartmented and multilevel modes of operation are essentially the same, there are some additional procedures required for the latter. The most significant difference is that the DCI is the accreditation authority for systems and networks operating in the multilevel mode. (UNCLASSIFIED)

ITER

Table 1

Security SAFEGUARDS by Mode of Operation

73%

SAFEGUARD	Dedicated	System High	Compartmented	Multilevel *
Access Control and Labels				
1. Discretionary Access Control	A	A	A	A
2. Object Reuse	—	—	A	A
3. Labels	A	A	A	A
4. Mandatory Access Control	A	A	A	A
Accountability				
5. Identification & Authentication	A	A	A	A
6. Identification of User Terminal	—	A	A	A
7. Trusted Path	—	A	A	A
8. Audit	—	A	A	A
Operational Assurance				
9. System Architecture	—	A	A	A
10. System Integrity	—	A	A	A
11. Trusted Facility Management	—	A	A	A
12. Trusted Recovery	—	—	A	A
Life Cycle Assurance				
13. Security Testing	—	A	A	A
14. Design Specification & Verification	—	—	A	A
15. Configuration Management	—	A	A	A
16. Trusted Distribution	—	A	A	A
Documentation				
17. System Security Statement/Plan	A	A	A	A
18. Security Features User's Guide	A	A	A	A
19. Trusted Facility Manual	—	A	A	A
20. Test Documentation	—	A	A	A
21. Design Documentation	—	—	A	A
Environmental Protection				
22. Communications Security (COMSEC)	A	A	A	A
23. Physical Security	A	A	A	A
24. TEMPEST	A	A	A	A
25. Personnel Security	A	A	A	A
Administrative				
26. Annual Accreditation	A	A	A	A
27. Dial-up Lines	A	A	A	A
28. Protection of Software	A	A	A	A
29. Access Authentication	A	A	A	A

Note: "A" means applicable to the identified modes of operation.

* Although the requirements for the compartmented and multilevel modes of operation are essentially the same, there are some additional procedures required for the latter. The most significant difference is that the DCI is the accreditation authority for systems and networks operating in the multilevel mode. (UNCLASSIFIED)

OS 18

Table 1

Security SAFEGUARDS by Mode of Operation

SAFEGUARD	Dedicated	System High	Compartmented	Multilevel *
Access Control and Labels				
1. Discretionary Access Control	A	A	A	A
2. Object Reuse	—	—	A	A
3. Labels	A	A	A	A
4. Mandatory Access Control	A	A	A	A
Accountability				
5. Identification & Authentication	A	A	A	A
6. Identification of User Terminal	—	A	A	A
7. Trusted Path	—	A	A	A
8. Audit	—	A	A	A
Operational Assurance				
9. System Architecture	—	A	A	A
10. System Integrity	—	A	A	A
11. Trusted Facility Management	—	A	A	A
12. Trusted Recovery	—	—	A	A
Life Cycle Assurance				
13. Security Testing	—	A	A	A
14. Design Specification & Verification	—	—	A	A
15. Configuration Management	—	A	A	A
16. Trusted Distribution	—	A	A	A
Documentation				
17. System Security Statement/Plan	A	A	A	A
18. Security Features User's Guide	A	A	A	A
19. Trusted Facility Manual	—	A	A	A
20. Test Documentation	—	A	A	A
21. Design Documentation	—	—	A	A
Environmental Protection				
22. Communications Security (COMSEC)	A	A	A	A
23. Physical Security	A	A	A	A
24. TEMPEST	A	A	A	A
25. Personnel Security	A	A	A	A
Administrative				
26. Annual Accreditation	A	A	A	A
27. Dial-up Lines	A	A	A	A
28. Protection of Software	A	A	A	A
29. Access Authentication	A	A	A	A

3.4
x
41
59

Note: "A" means applicable to the identified modes of operation.

* Although the requirements for the compartmented and multilevel modes of operation are essentially the same, there are some additional procedures required for the latter. The most significant difference is that the DCI is the accreditation authority for systems and networks operating in the multilevel mode. (UNCLASSIFIED)